CSE 345/545: Foundations to Computer Security

HOMEWORK ASSIGNMENT 1 (TOTAL OF 100 POINTS)

Due by 23:59hrs on Aug 29, 2019

Plagiarism policies will be strictly enforced.

Part I [10 points]

Classify the below-mentioned passwords as very strong, strong, neutral, weak, very weak and also, justify your reasoning. Please keep the response within 20 words for each.

1. 1q2w3e4r5t
2. Football
3. 983749587
4. 4><8mM%
5. FCSPassword1
6. &*^)&@_(%$
7. SecurePassword@123
8. monkey
9. Hello!
10. Qwertyuiop

Part II [30 points]

Design an authentication, authorization and identification scheme for visitors, customers, and employees of a Bank.

- Describe the complete design of the system and how each of the components will be incorporated?
- Discuss various (at least 3) ways in which an attacker might try to spoof the system.
- Give countermeasures that you have taken to avoid the spoofing and other attacks.

Please keep your complete response within 600–900 words.

Part III [45 points]

1) **[30 points]** Decipher the following Ciphertext

   ```
   ohgjungvernyylarrqgbgnyxgbhnobhgvfgursylvatfnhfntrvapvqragvqba'gguvaxv
   gnyxrqgbhnobhgguvfohghernyylfubhyqxabjgungvnzfrpergylnsylvatfnhfntrabg
   baylnzvnsylvatfnhfntrohgvnzgursylvatfnhfntrgunggbbxgurjnyxvatpurrfrohetr
   efcvpxyrfgurlVfubhyqVerznxrVfrnfbaVavarVbsVtnzrVbsVguebarf
   ```

   - Provide the plain text.
   - Provide working code for reversing this. You may choose any language to do so.
   - Describe the methodology, in detail, used for reversing the ciphertext.

- The original ciphertext in this question was modified by a TA by appending some random ciphertext at its end. Identify the randomly added ciphertext. Which security policy is violated in this case and why? (Explain in max 2 sentences)

Hint: It’s one of the ciphers covered in class.
Please keep your complete response concise and to the point.

2) **[15 points]** Write a program (in any language) to decrypt the below ciphertext which was encrypted using Substitution cipher with the key- “qpalzmxncbvksjdhfgwoeiruty”

```
Onz ocxzg cw onz kqgxzwo whzaczw qsdjx onz Mzkclqz qjl akqwwcmczl cj onz
xzjew Hqjonzgq. Co cw sdwo gzadxjcwqpkz mdg cow lqgv izgocaqk wogchzw dj
gzllcwn-dgqjxz meg rcon q kcxnozg ejlzgwclz. Co cw qj qhzu hgzlqodg,
hgcsqgckt hgztcjx dj ejxekqozw wean qw lzzg qjl rckl pdqg.
```

Part IV [15 points]
Suggest ways to make the IIITD Authentication System more usable. Address the topics that we discussed in class. Answer the question in less than 450 words. In your proposed system, please discuss:

- What usability issues you feel need to be addressed?
- Include some suggestions to improve the system.

Remember there is a trade-off, the scheme should provide reasonable security at least.

Submission guidelines (points will be deducted if not followed):

All the codes/pdf files must be compressed in a zip file which is to be uploaded to the Google classroom deadline. Instructions to run the code must also be included (in a text file called ‘instructions’).
Do not send any assignment by email! No email submissions will be entertained.
FileName : A1_ROLLNO.zip